REMARKS

Applicant respectfully requests the Examiner's reconsideration of the present application as amended.

Claims 1-25 are pending in the present application.

Claims 20-22 are rejected under 35 U.S.C. §101 because the claimed invention is indicated to be directed to non-statutory subject matter.

Claims 1-6 and 20-25 are rejected under 35 U.S.C. §103(a) as being unpatentable over US Patent No. 4,962,449 ("Schlesinger") in view of US Patent No. 7,228,563 ("Szor").

Claims 7-19 are rejected under 35 U.S.C. §103(a) as being unpatentable over Schlesinger in view of Szor, and further in view of US Patent No. 7,080,405 ("Himmel").

Claims 1, 8, 14, and 20-23 have been amended.

Claims 26 and 27 have been added.

Support for amended claims 1, 8, 14, 20, and 23 is found on page 8, 12, 13, and 16.

Support for new claims 26 and 27 is found on pages 5 and 13 respectively.

No new matter has been added.

Claims 20-22 are rejected under 35 U.S.C. §101. Specifically, the Office Action mailed 6/28/2007 states

> Since Applicant's specification states that the term "machine readable medium" includes carrier waves (see Specification, p. 15, line 25 to p. 16, line 3), which are intangible, the claims there encompass non-statutory subject matter.

(6/28/2007 Office Action, p2).

Applicant submits that claim 20-22 have been amended to claim "disk" instead of "machine readable medium". Applicant submits that since a disk is statutory subject matter, the rejection under 35 U.S.C. §101 has been overcome in view of the amendments.

Claims 1-25 are rejected under 35 U.S.C. §103(a) as being unpatentable over Schlesinger, Szor, and Himmel.

Applicant submits that claims 1-27, as amended, are patentable over Schlesinger, Szor, and Himmel under 35 U.S.C. §103(a).

Schlesinger includes a disclosure of an apparatus provided that enables a computer system access procedure to be secure from hackers and other potential unauthorized computer system users. The invention's features include a switchboard, a centralized security interface, which interacts with a location recognition device at each remote location. Security is provided by secure and easily changeable location recognition device initialization, the transmission of a unique location security code from each location recognition device to the switchboard, and location recognition device immobility through the use of volatile memory. Unauthorized computer system access is prevented by a switchboard access protocol that uses a relationship between location security codes and personal identification codes to limit specific computer system users to specific remote locations and to lock-out, from computer system access, any remote location or analog thereof that the switchboard determines is being used by a hacker or other unauthorized user.

Szor includes a disclosure of hooking a critical operating system function, originating a call to the critical operating system function with a call module of a parent application, stalling the call, determining a location of the call module in memory, and determining whether the location is in an executable area of the memory. Upon a determination that the call module is not in the executable area, the method further includes terminating the call. By terminating the call, execution of a child application that would otherwise allow unauthorized remote access is prevented (see Szor Abstract).

Himmel includes a disclosure of a system, method and computer program product that send wireless control messages to electronic devices, such as audio and video recorders, cameras, radios, televisions, mobile phones, portable or handheld computers and personal digital assistants, that have come within an environment or that are in an environment that changes. In such an environment, a wireless receiver in the mobile electronic device receives the control messages. In a hardware implementation, electronic gates are set to disable the one or more features of the device. In a software implementation,

current power status flags are set in a memory device within the mobile electronic device to a reduced power setting. Outside the environment, the electronic gates or power status flags revert to full power. The device driver for each feature of the mobile electronic device will reject I/O operations inconsistent with the current power status flags for that feature (see Himmel Abstract).

Applicant submits that Schleiser, Szor, and Himmel do not teach or suggest synchronizing data in a database on a client system in response to location information about the client system, and transmitting a trigger signal to the client system that prompts the client system to present the data from the database and to lock the client system to prevent a user from using the client system to perform regular computing operations in response to determining a relevance of an event to a location of the client system.

The Office Action mailed 6/28/2007 states in part that

> As per claims 1, 4, and 23-25 Schlesinger discloses a computer security system in which a switch board (the server) regulates an LRD workstation (the client). The server may send the client location registration information, an LSC (derived from the client's location ID), thereby synchronizing the client's database (see column 7, line 48 to column 8, line 14). The server later uses the client information in handling a login attempt (an event) and locks it out if the information is incorrect, determining the client's information to be comprised and thus irrelevant (see column 9, line 39 to column 10, line 40).

(9/28/2007 Office Action, p. 3) (Emphasis Added).

On the contrary, applicant submits that the "LSC" which the Office refers to is a "location security code" (see Schlesinger column 3, lines 61-63). The location security code is loaded into a location recognition device (LRD) 2 by a switchboard 1 in a secure area 6 during LRD initialization (see Schlesinger column 7, lines 34 through column 8, line 25 and Figure 1). The location security code is transmitted back to the switchboard 1 when access to a computer 4 in the secure area 6. The switch board 1 determines whether the transmitted location security code is authorized (see Schlesinger column 9, lines 46-63 and Figure 1). The location security code is not presented by a client system in response to determining a relevance of an event to a location of the client system.

Furthermore, the "lock-out" referred to by the Office and described in Schlesinger refers only to preventing access to components in a secure area (6) not to locking out a workstation from its own resources. Schlesinger describes "lock-out" as the switchboard's (1) refusal to allow access to the computer (4) and storage device (5) in a secure area (6) to a workstation (7) (see Schlesinger column 10, lines 38-40). Schlesinger does not describe locking a client system to prevent a user from using the client system to perform regular computing operation.

In addition, Schlesinger "locks-out" a workstation (7) after some specified number of unauthorized "personal identification code" (PIC) entries regardless of the location of the workstation (7) (see Schlesinger column 10, lines 31-38). Schlesinger does not lock-out a workstation in response to determining a relevance of an event to a location of the client system.

Szor only discloses a shell code blocking system and method. Szor does not teach or suggest synchronizing data in a database on a client system in response to location information about the client system, and transmitting a trigger signal to the client system that prompts the client system to present the data from the database and to lock the client system to prevent a user from using the client system to perform regular computing operations in response to determining a relevance of an event to a location of the client system.

Himmel only discloses sending wireless control messages that limit device function. Himmel does not teach or suggest synchronizing data in a database on a client system in response to location information about the client system, and transmitting a trigger signal to the client system that prompts the client system to present the data from the database and to lock the client system to prevent a user from using the client system to perform regular computing operations in response to determining a relevance of an event to a location of the client system.

In contrast, claim 1, as amended states

> A method for managing data, comprising:
> synchronizing data in a database on a client system in response to location information about the client system; and

> transmitting a trigger signal to the client system that prompts the client system to present the data from the database and to lock the client system to prevent a user from using the client system to perform regular computing operations in response to determining a relevance of an event to a location of the client system.

(Claim 1, as Amended) (Emphasis Added).

Claim 20 and 23 include similar limitations. Claim 8 includes the limitations of synchronizing data in databases, and presenting the data and locking the client system to prevent a user from using the client system. Claim 14 includes the limitation of locking the client system to prevent a user from using the client system. Given that claims 2-7, and 26-27 are dependent on claim 1, claims 9-13 are dependent on claim 8, claims 15-19 are dependent on claim 14, claims 21-22 are dependent on claim 20, and claims 24-25 are dependent on claim 23, it is likewise submitted that claims 2-7, 9-13, 15-19, 21-22, 24-25, and 26-27 are also patentable over Schlesinger, Szor, and Himmel under 35 U.S.C. § 103(a).

Applicant submits that Schleiser, Szor, and Himmel also do not teach or suggest synchronizing data in databases on client systems that include computer systems capable of processing data in response to location information from the client systems, and broadcasting a trigger signal with a location tag that prompts a client system at a location that matches the location tag to present the data from its database and to lock the client system to prevent a user from using the client system to perform regular computing operations, wherein the trigger signal is broadcasted to all client systems regardless of whether they are at a location that matches the location tag.

The Office Action mailed 9/28/2007 states in part that

> Claims 7-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 4,962,449 to Schlesinger in view of U.S. Patent No. 7,228,563 to Szor as applied to claim 1 et al above, and further in view of U.S. Patent No. 7,080,405 to Himmel et al.
>
> Although Schlesinger and Szor disclose support for mobile clients (see column 8, lines 54-62), Schlesinger only discloses

> the use of a network over fixed telephone lines, rather than using wireless connectors, as is common in mobile computers.
>
> Himmel discloses network management over a wireless network wherein clients are controlled via wireless messages (see column 3, lines 36-44) to all units in the environment (i.e. in range) (see column 4, lines 15-21) and control messages may be broadcast to all units in a location (see column 3, line 65 to column 4, line 1) I order to limit uses of all devices in a facility.

(6/28/2007 Office Action, pp. 4-5).

On the contrary, applicant submits that Himmel discloses broadcasting a wireless control message to electronic devices that have come within a given range or an environment (see Himmel column 3, lines 36-38). All electronic devices that detect the power control message sets current status flags for features specified to be controlled (see Himmel Figure 8 block 212 and 220 and Figure 10 block 212 and 252). Himmel does not teach or suggest broadcasting a trigger signal with a location tag that locks the client system if the client system is at a location that matches the location tag. In fact, Himmel does not provide any disclosure or reference to a location tag being broadcasted with its control message.

Furthermore, as stated earlier, applicant submits that the "LSC" which the Office refers to is a "location security code" (see Schlesinger column 3, lines 61-63). The location security code is loaded into a location recognition device (LRD) 2 by a switchboard 1 in a secure area 6 during LRD initialization (see Schlesinger column 7, lines 34 through column 8, line 25 and Figure 1). The location security code is transmitted back to the switchboard 1 when access to a computer 4 in the secure area 6. The switch board 1 determines whether the transmitted location security code is authorized (see Schlesinger column 9, lines 46-63 and Figure 1). The location security code is not presented by a client system in response to determining a relevance of an event to a location of the client system.

In addition, as stated earlier, the "lock-out" referred to by the Office and described in Schlesinger refers only to preventing access to components in a secure area (6) not to locking out a workstation from its own resources. Schlesinger describes "lock-out" as the switchboard's (1) refusal to allow access to the computer (4) and storage device (5) in a secure area (6) to a workstation (7) (see Schlesinger column 10,

lines 38-40). Schlesinger does not describe locking a client system to prevent a user from using the client system to perform regular computing operation.

Moreover, as stated earlier, Schlesinger "locks-out" a workstation (7) after some specified number of unauthorized "personal identification code" (PIC) entries regardless of the location of the workstation (7) (see Schlesinger column 10, lines 31-38). Schlesinger does not lock-out a client system in response to determining that a client system is at a location that matches the location tag.

In contrast, claim 8 as amended states

> A method for managing data, comprising:
> synchronizing data in databases on client systems that include computer systems capable of processing data in response to location information from the client systems; and
> broadcasting a trigger signal with a location tag that prompts a client system at a location that matches the location tag to present the data from its database and to lock the client system to prevent a user from using the client system to perform regular computing operations, wherein the trigger signal is broadcasted to all client systems regardless of whether they are at a location that matches the location tag.

(Claim 8, as Amended) (Emphasis Added).

Given that claims 9-13 depends on claim 8, it is likewise submitted that claims 9-13 are also patentable over Schlesinger, Szor, and Himmel under 35 U.S.C. § 103(a).

In view of the arguments set forth herein, it is respectfully submitted that the applicable rejections and have been overcome. Accordingly, it is respectfully submitted that claims 1-27 should be found to be in condition for allowance.

The Examiner is invited to telephone Applicant's attorney (217-377-2500) to facilitate prosecution of this application.

If any additional fee is required, please charge Deposit Account No. 50-4238.

Respectfully submitted,

Date September 28, 2007

Lawrence M. Cho
Attorney for Applicant
Registration No. 39,942

CERTIFICATE UNDER 37 CFR 1.8: The undersigned hereby certifies that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail, in an envelope addressed to: Mail Stop Amendment, Commissioner of Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on this 28th day of 2007.

Cheryl Schwartz

Name

Signature